FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

Cybersecurity skills & workforce gap: le iniziative di Cyber 4.0

Alessandro Calabrese
Responsabile Formazione e Advisory, Cyber 4.0
alessandro.calabrese@cyber40.it

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

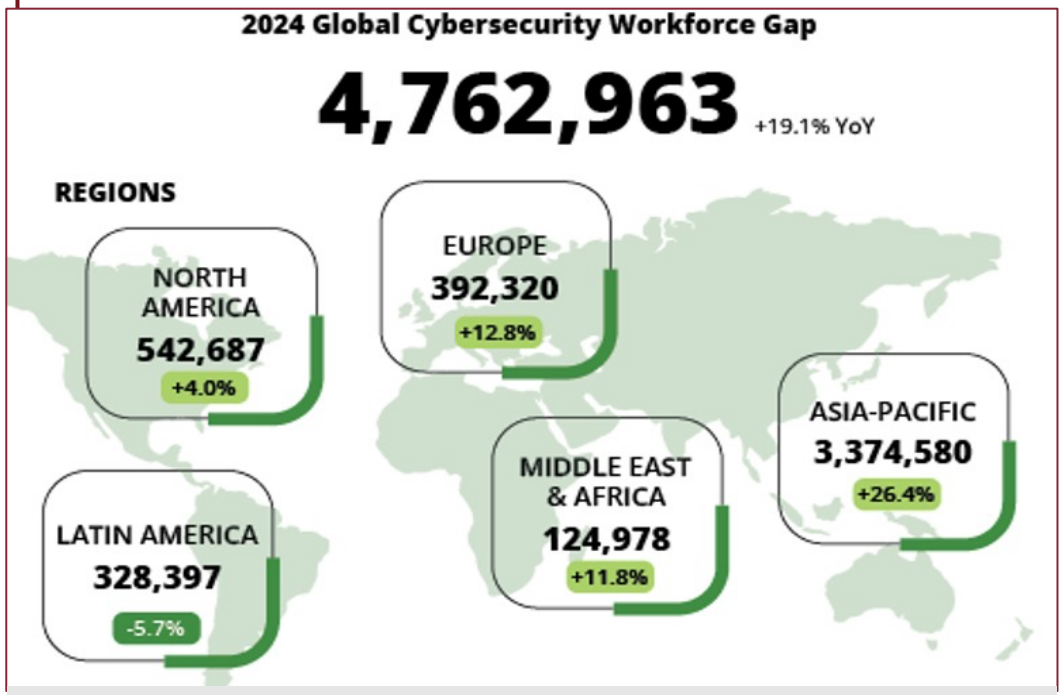
Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

Cybersecurity Skills Gap: Europe 2025

FORUM 2025 CYBER 4.0

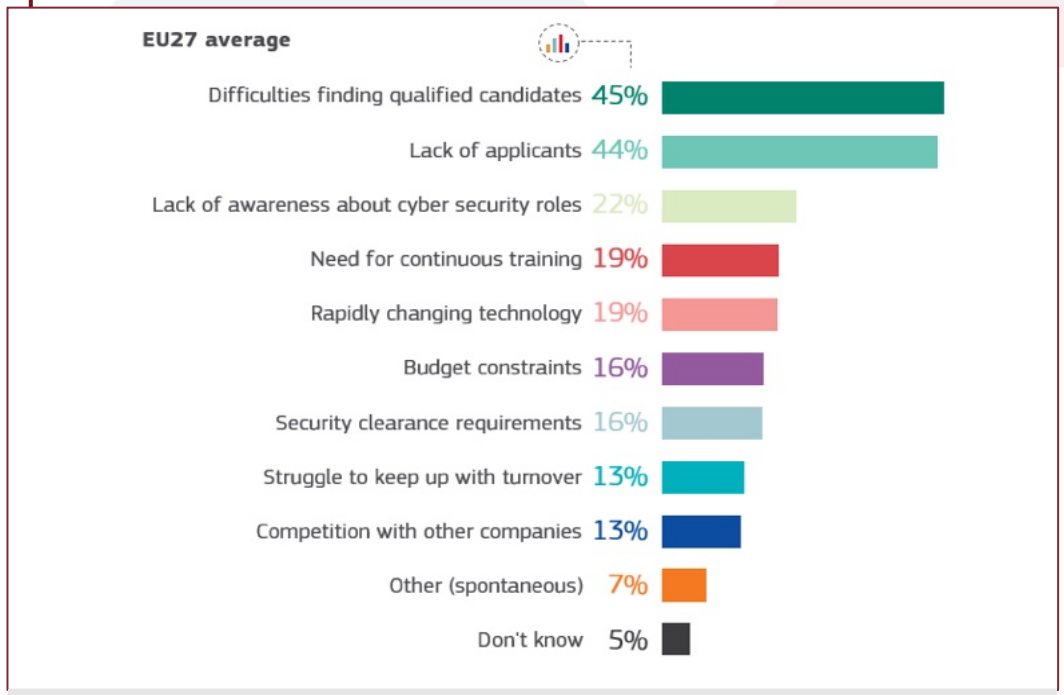
CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

- Il gap della forza lavoro in ambito cybersecurity a livello globale nel 2024 si attesta a oltre **4,5 milioni posti di lavoro**, di cui quasi **400mila in Europa.**



Questo divario è destinato a crescere con l'entrata in vigore di normative come **NIS2**, **Cyber Resilience Act** e **DORA**.

- Secondo l'Eurobarometro 2024, **l'81%** delle aziende ritiene che le difficoltà di assunzione in cybersecurity aumentino il rischio di attacchi.



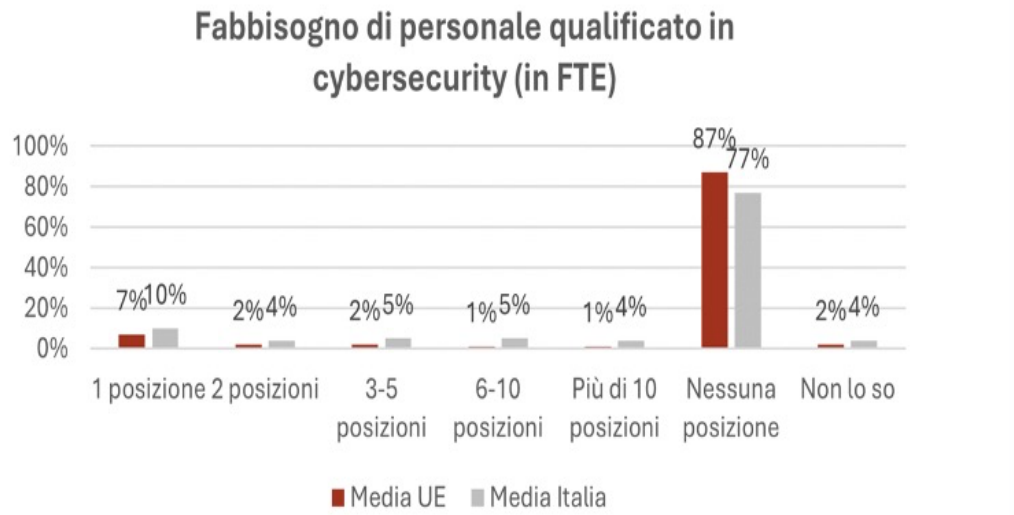
Inoltre, **il 76%** degli addetti non possiede qualifiche formali, e nel settore sanitario ed educativo, **il 66%** dei ruoli in cybersecurity è coperto da personale proveniente da altri ambiti professionali.

Cybersecurity Skills Gap: Italia 2025

FORUM 2025 CYBER 4.0

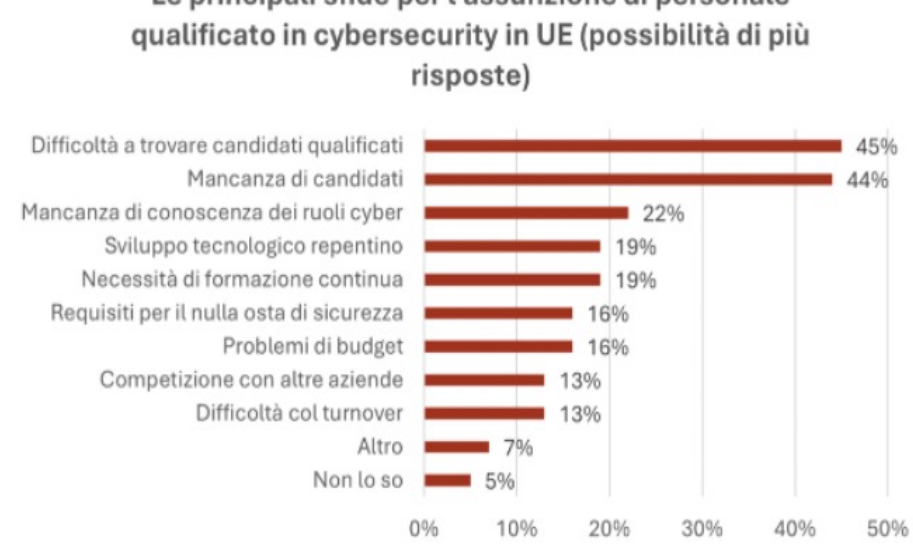
CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

- Anche **in Italia**, il divario di competenze in cybersecurity è un problema critico che ostacola la capacità di risposta agli attacchi informatici.



Fonte: Eurobarometer, Cyberskills, maggio 2024

- Il Rapporto Clusit 2025 evidenzia come il nostro Paese sia tra i più colpiti al mondo, con un **incremento del 15%** degli incidenti rispetto al 2023.



Fonte: Eurobarometer, Cyberskills, maggio 2024

EUROPEAN CYBERSECURITY SKILLS FRAMEWORK

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

ECSF

*Framework di riferimento UE per l'identificazione delle **competenze** e delle **figure professionali** in ambito cybersicurezza, sviluppato da ENISA.*

Profili Professionali

L'ECSF identifica **12 ruoli fondamentali** nel settore della cybersecurity, ognuno con **specifiche responsabilità operative.**
Questi coprono tutte le funzioni critiche per garantire la sicurezza digitale in organizzazioni di ogni dimensione.

Competenze e Abilità

Per ciascun ruolo, il framework dettaglia le **competenze tecniche** (hard skill) **richieste**, come gestione delle vulnerabilità o incident response, e **le competenze trasversali** (soft skill), come problem solving, pensiero critico e capacità comunicative.

Formazione e Certificazioni

L'ECSF suggerisce un **collegamento diretto** tra ruoli professionali e percorsi formativi, indicando le certificazioni più rilevanti (es. CISSP, CEH, ISO 27001). Questo favorisce la costruzione di percorsi di carriera coerenti e misurabili.

Il ruolo di Cyber 4.0 nel WG ECSF

Product Security Updating

*Cyber 4.0 collabora all'ECSF come **osservatore permanente**, e prende parte attivamente al **Working Group ECSF 2023–2025** per supportare adozione e sviluppo del framework.*

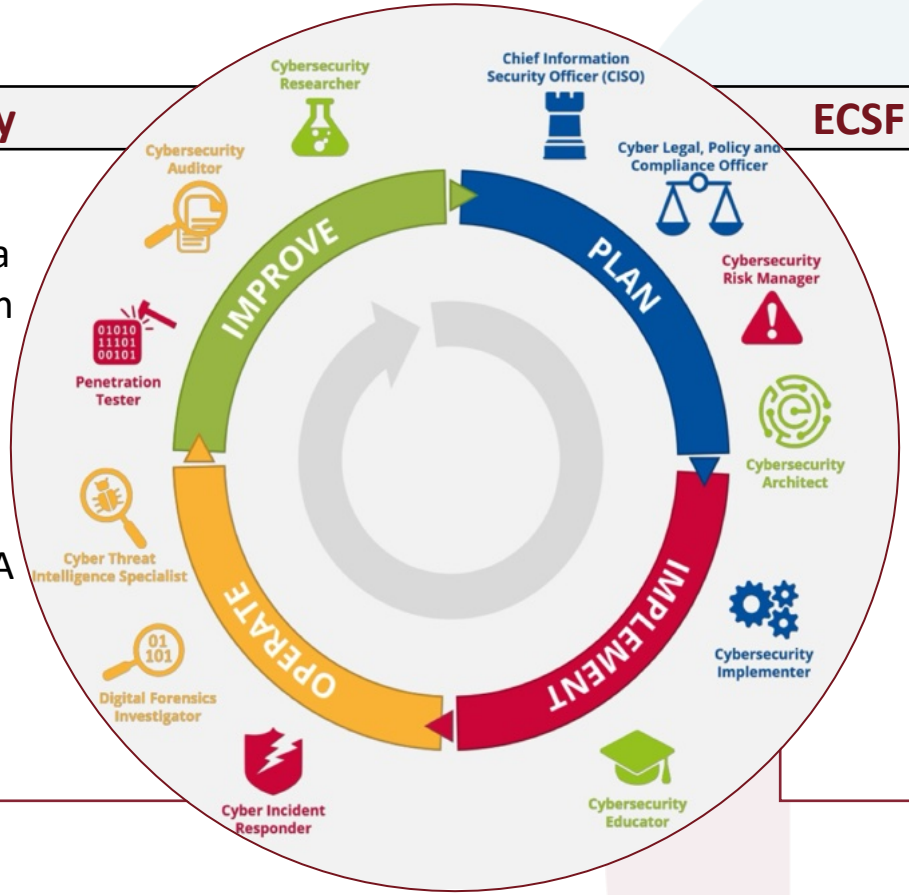
Revisione ECSF: Product Security

Obiettivo

Revisione del framework ECSF in ottica allineata agli adempimenti del CRA con **focus sulla sicurezza dei prodotti digitali e della catena di produzione**.

Metodo

Analisi degli obblighi normativi del CRA associandoli ai **ruoli ECSF più idonei e alle rispettive task, conoscenze e competenze.**



ECSF Product Security: use case SPACE

Obiettivo

Allineare framework ECSF allo **sviluppo sicuro dei prodotti digitali** nel **settore spaziale.**

Metodo

Analisi dei **ruoli** cybersecurity rilevanti nel settore spaziale;
Mappatura dei **requisiti** ECSF già esistenti;
Identificazione di **gap e integrazioni** tramite interviste con esperti del settore.

Cyber 4.0: un osservatorio nazionale per cybersecurity skills & needs

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Cyber 4.0 ha avviato una iniziativa di ricerca che mira a realizzare una versione italiana del **Report Cybersecurity Skills Needs Analysis di CyberHubs,** integrando in aggiunta statistiche sugli **impatti delle normative** in fase di adozione e sul **fabbisogno cyber** delle **PMI italiane.**

Action Plan

1. **Individuazione enti e imprese**
2. **Individuazione stakeholder e partner**
3. Invio del **questionario**
4. Raccolta **dati anonima e aggregata**
5. **Workshop & webinar**
6. Redazione di un primo **report** 2025
7. **Presentazione pubblica**

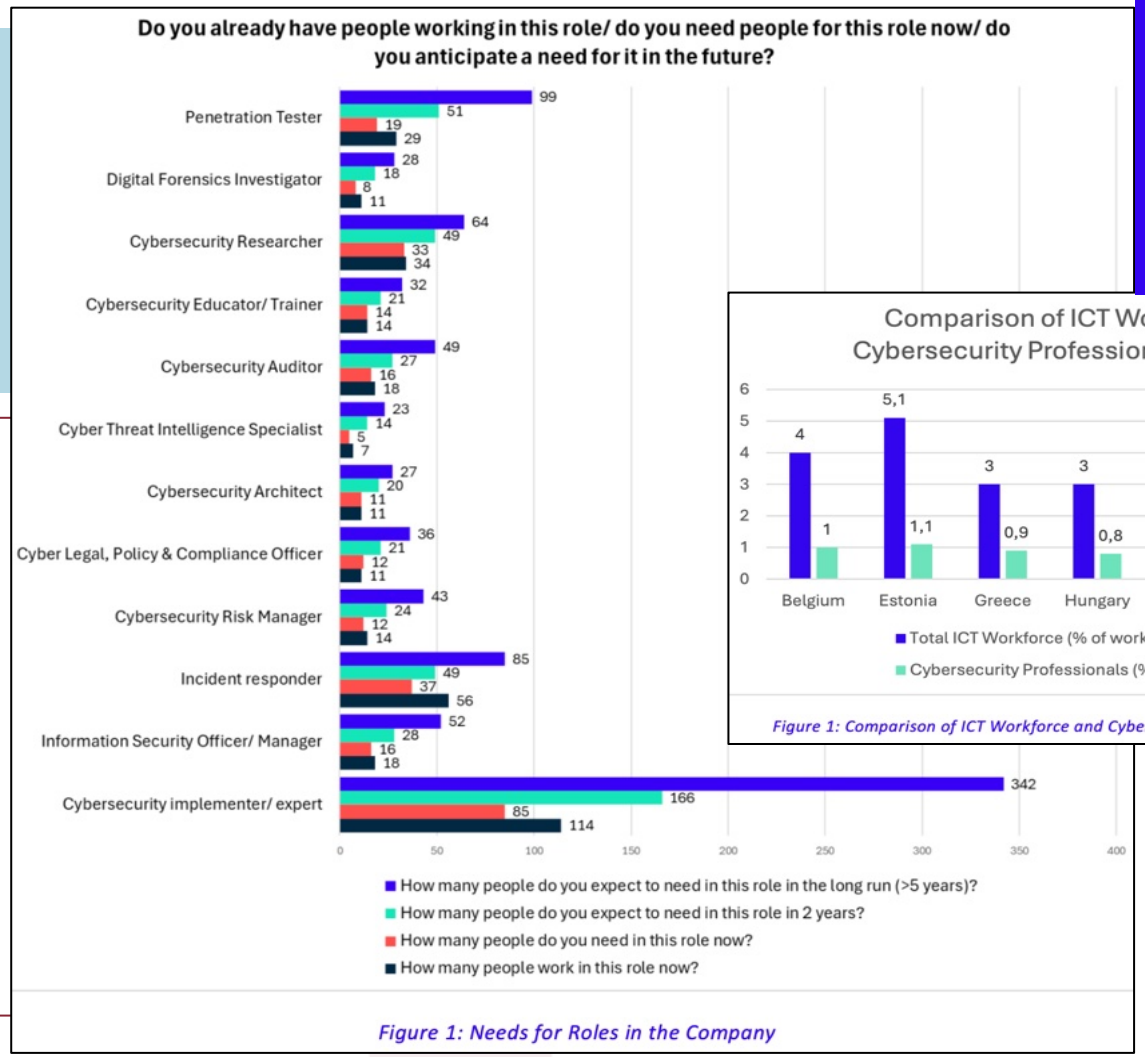


Figure 1: Needs for Roles in the Company

CyberHubs

Cybersecurity Skills Needs Analysis Summary Report.

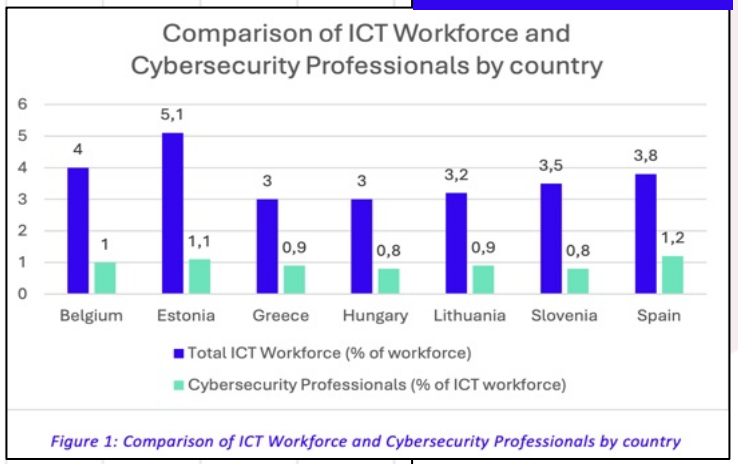


Figure 1: Comparison of ICT Workforce and Cybersecurity Professionals by country

L’analisi di Cyber 4.0

Main Output: Report nazionale Cybersecurity Skills Needs Analysis

Una fotografia aggiornata della **domanda / offerta di competenze** in cybersecurity.

Topic Principali

1. **Statistiche Workforce & Skill gap** sulle PMI italiane
2. **Ruoli, responsabilità** e modelli organizzativi
3. **Best practice** per il rafforzamento delle competenze cyber

Articoli di approfondimento

1. **Confronto occupazionale** tra percorsi ITS e universitari
2. Impatto della **Direttiva NIS-2 e del CRA** sugli investimenti cybersecurity delle PMI

Obiettivi a lungo termine

Offrire uno strumento di **osservazione nazionale**;

Supportare le PMI nel rafforzamento delle competenze interne;

Migliorare la sinergia tra **mondo della formazione e imprese.**

Il Questionario

La tua opinione conta: utilizza il QR code per compilare il questionario

Aggiornamento Vademecum sulla Cybersecurity per le PMI

Nel 2023 Cyber 4.0, in collaborazione con Unindustria e con l'endorsement del MIMIT e di ENISA, ha realizzato il "Vademecum sulla Cybersecurity per le PMI".

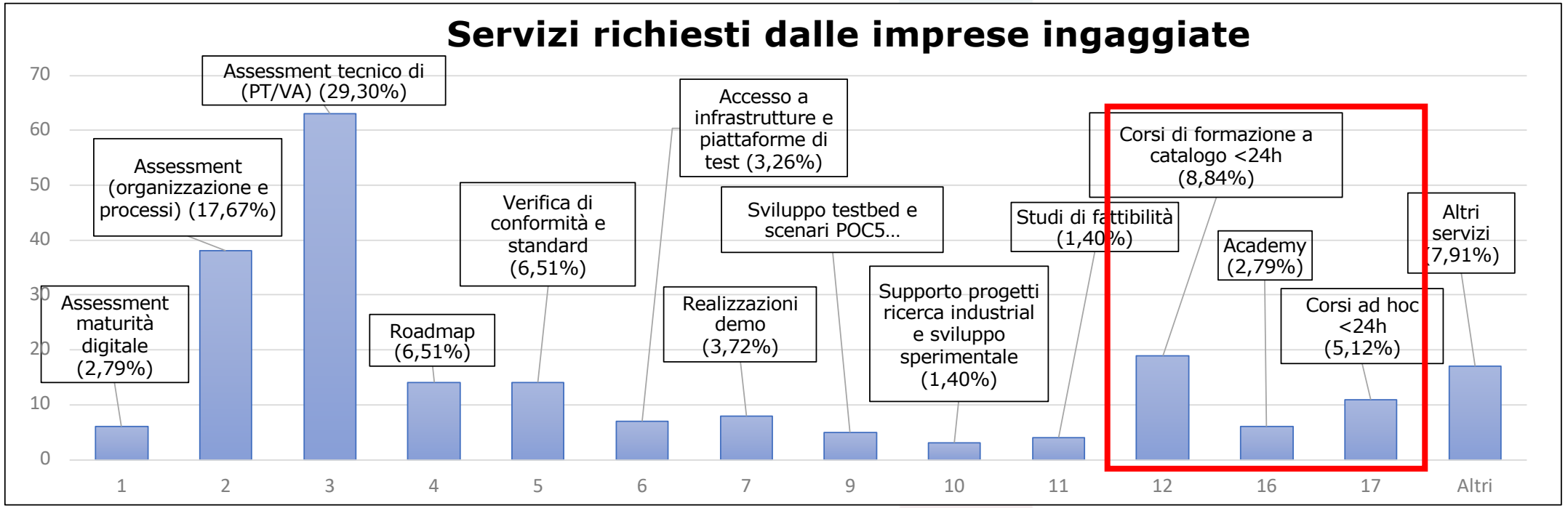
In corso l'aggiornamento del Vademecum.

- **AI Management Systems**
- **Evoluzione della Minaccia Cyber**
- **Product Security Management (OT & IoT)**
- **Supply Chain Security Management**
- **Aggiornamento normativo (NIS2; CRA; AI Act …)**
- **NextGen Cybersecurity Solutions**

Servizi di Formazione Finanziati PNRR:
I risultati del 2024

Le attività di formazione rappresentano il **secondo servizio finanziato maggiormente richiesto ed erogato** dopo le attività di Assessment, su un totale di 7 servizi

Dimensione	Imprese ingaggiate	%
Piccole	82	53,6%
Medie	54	35,3%
Grandi	17	11,1%
Totale	**153**	



I progetti di Formazione extra PNRR (1/2)

FORUM 2025 CYBER 4.0

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

MINISTERO DELL'AMBIENTE E DELLA SICUREZZA ENERGETICA

Ministero delle Imprese e del Made in Italy

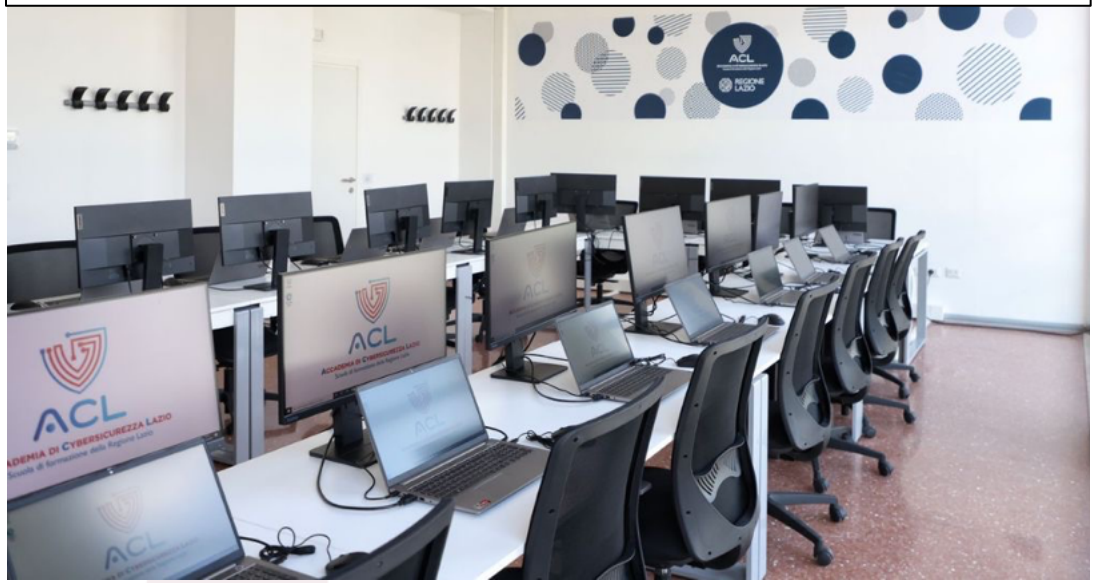
DINTEC
CONSORZIO PER L'INNOVAZIONE TECNOLOGICA

punto impresa digitale

CAMERA DI COMMERCIO DELL'EMILIA

I progetti di Formazione extra PNRR (2/2)

ACL
ACCADEMIA DI CYBERSICUREZZA LAZIO
Scuola di formazione della Regione Lazio



FORUM 2025
CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Diffusione e certificazione delle competenze cyber

Antonio Capobianco
CEO, Fata Informatica

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea
NextGenerationEU

Hosted by:
ROMA TRE
UNIVERSITÀ DEGLI STUDI

FORUM 2025 CYBER 4.0

ROMA TRE Aula Magna Rettorato
4 - 5 Giugno 2025

CYBER 4.0 CYBERSECURITY COMPETENCE CENTER

Cyber competence gap, qualcosa è cambiato

Cybersecurity Virtual Escape Room for Awareness

Prof. Mattia Siciliano – Luiss Business School S.p.A – mattia.siciliano@luissbusinessschool.it
Ing. Piero Fioretti – CEO Versy srl – piero@versytechnolgies.com

Con il patrocinio di:

Ministero delle Imprese e del Made in Italy

Sotto l'alto patrocinio del Parlamento europeo

Finanziato dall'Unione europea NextGenerationEU

Hosted by:

ROMA TRE UNIVERSITÀ DEGLI STUDI

Cyber competence gap, qualcosa è cambiato

Cybersecurity Virtual Escape Room for Awareness

The human factor represents the main vulnerability for SMEs in the cyber context.

Cyberattacks increasingly exploit users' lack of awareness or limited knowledge of digital risks, thereby gaining unauthorized access to company systems.

For this reason, even within the framework of initiatives promoted by the CTEs, **it is advisable to adopt innovative strategies that go beyond traditional training, engaging users and the entrepreneurial fabric through interactive and technologically advanced approaches**.

Cyber competence gap, qualcosa è cambiato

Cybersecurity Virtual Escape Room - Project Scope

The goal of the project is to study the conditions and content aimed at implementing an innovative virtual environment, represented by an Escape Room.

The design approach adopted is action research: the data collected during the design phase and from user simulations will be analyzed to explore behavioral and cybersecurity management aspects.

This virtual environment is designed to facilitate the learning of fundamental cybersecurity principles through the simulation of crisis scenarios.

The experience will feature a **combination of interactive quizzes and a series of logical challenges** within an escape room environment, **placing users in situations that stimulate curiosity, challenge, and adrenaline.**

Cyber competence gap, qualcosa è cambiato

What is Virtual Environment

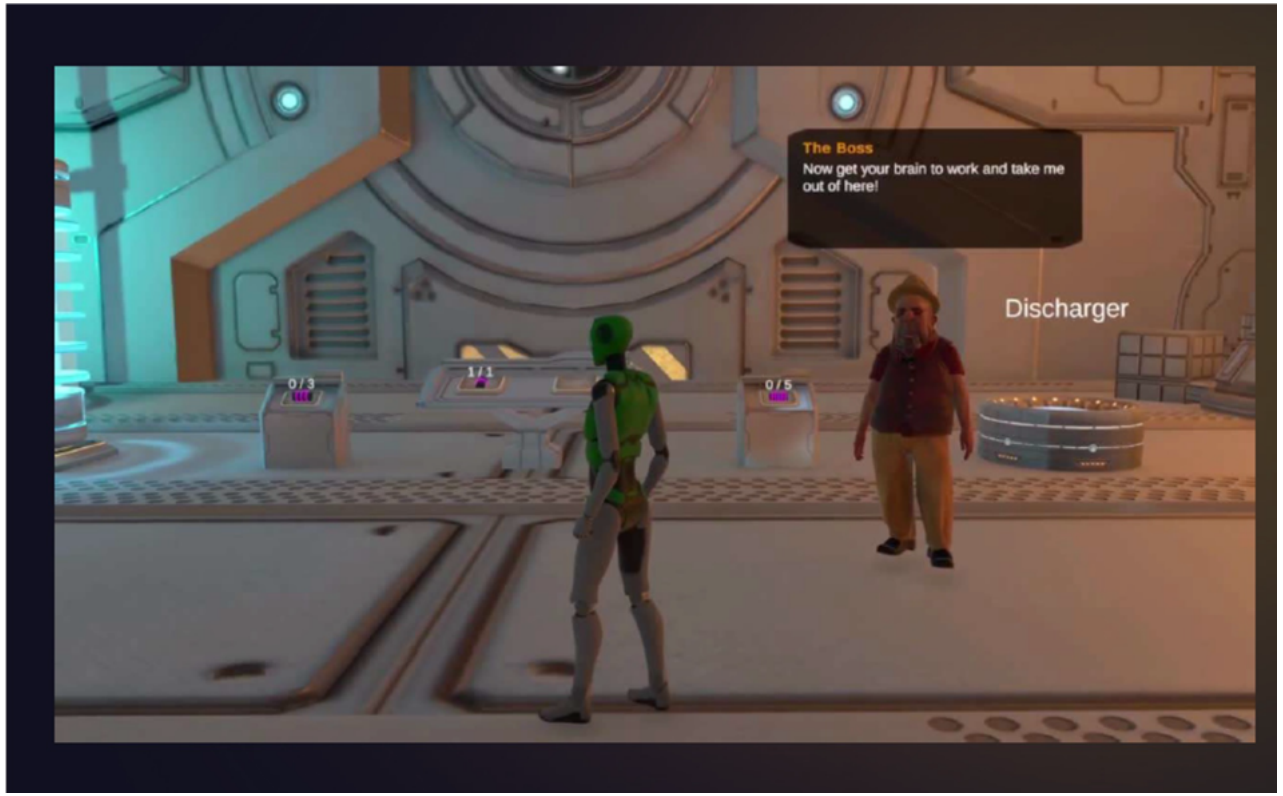
New UI
It's a new UI that uses AR, VR, virtual worlds and **games as means for the user to interact with the environment**

Emotional
Scalable as digital, immersive and captivating as physical

More Data
Unlocks a completely new set of **spatial data** that enhances the omnichannel approach of today

Cyber competence gap, qualcosa è cambiato

Pratical Use Cases : Training through the Virtual Escape Room



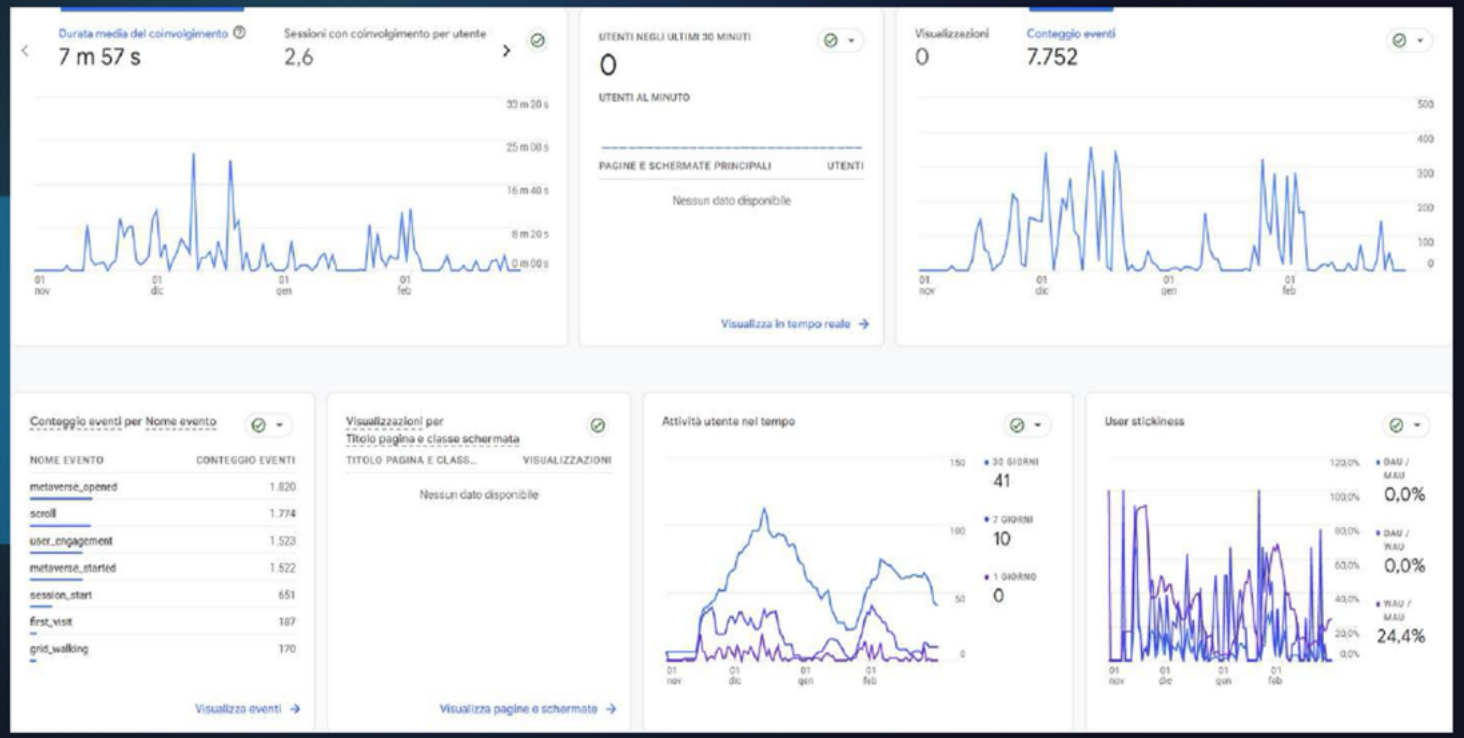
Virtual Training - Escape Room

- The candidate goes through a series of **tests** like in a Escape Room, each one producing **data** about different traits of the candidate.
- It's a **non-anxious setting** for the candidate, which brings more solidity to the outcome.
- It's an opportunity for the company to make **storytelling** and recount their vision, mission and values

Cyber competence gap, qualcosa è cambiato
Data Analytics

Engagement is a measure of how invested users are in an experience. Highly engaged users represent the core user base and are more likely to become paying users.

- Daily active Users
- New Users
- Number of User Sessions
- Total time spent
- Monthly active Users
- Average Session Time

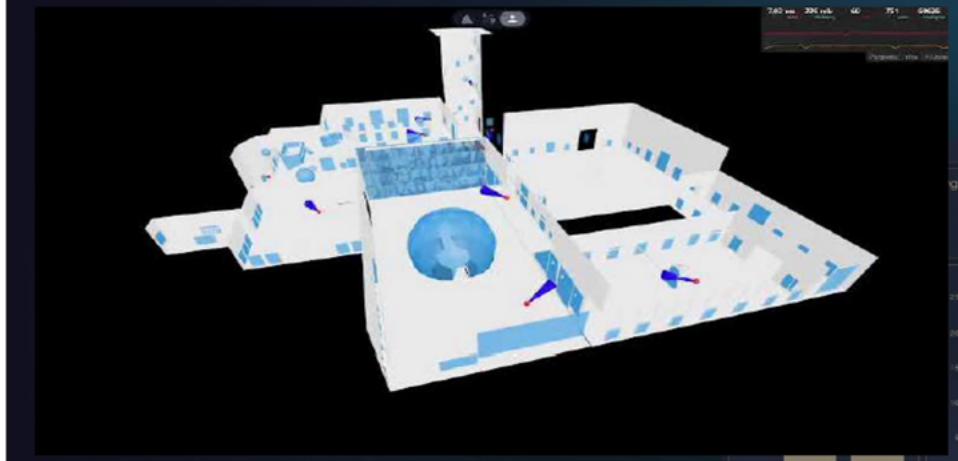


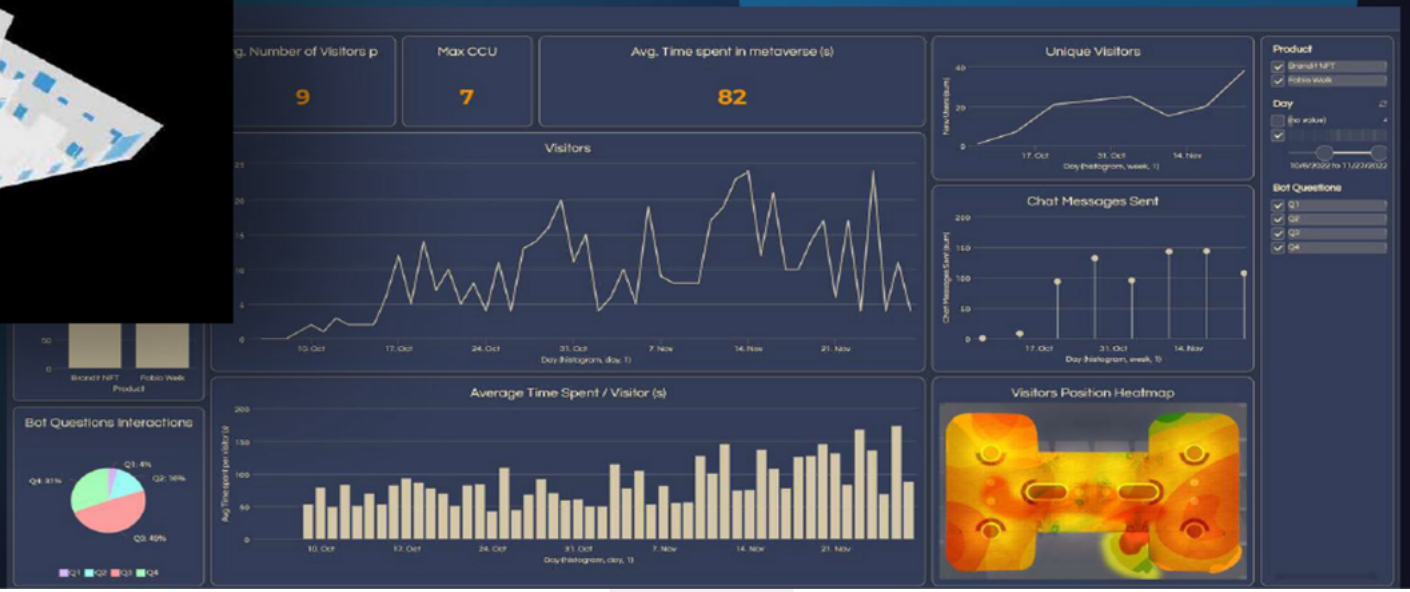
Cyber competence gap, qualcosa è cambiato

Data Analytics – Position and view Tracking

Discover how the audience uses the experiences with respect to space, view and time.

- Position in the space wrt time
- Networking activities
- Where people tend to look and for how long
- Heatmaps
- ...





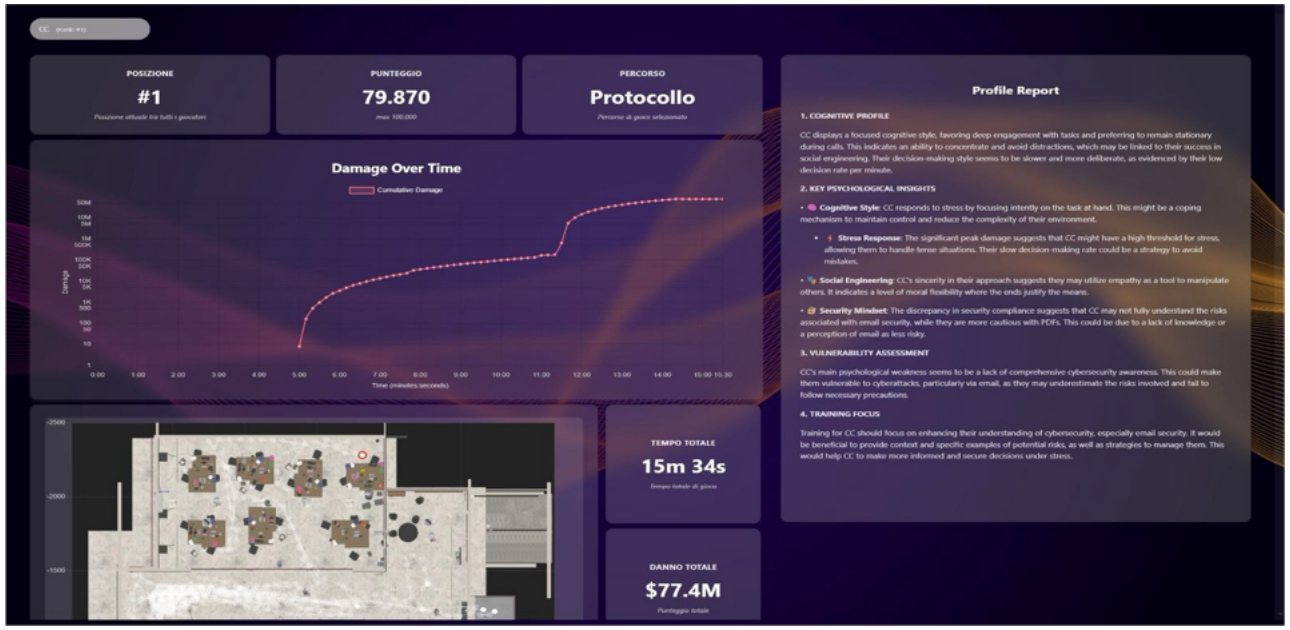
Cyber competence gap, qualcosa è cambiato

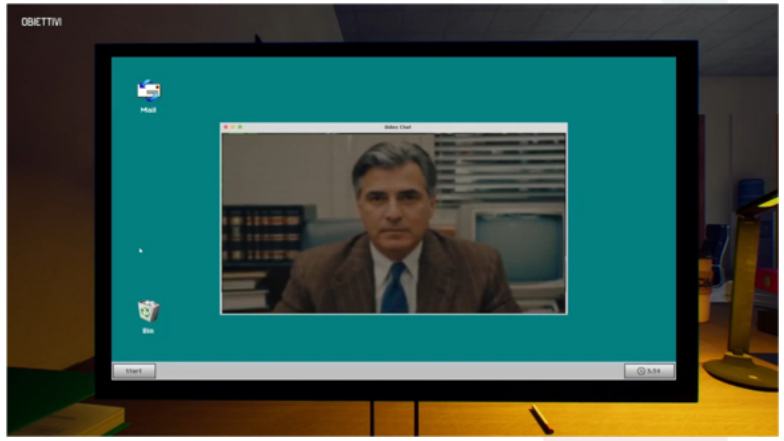
Trailer Virtual Escape Room

The simulation sees an employee fall in a phishing trap through a CFO attack.

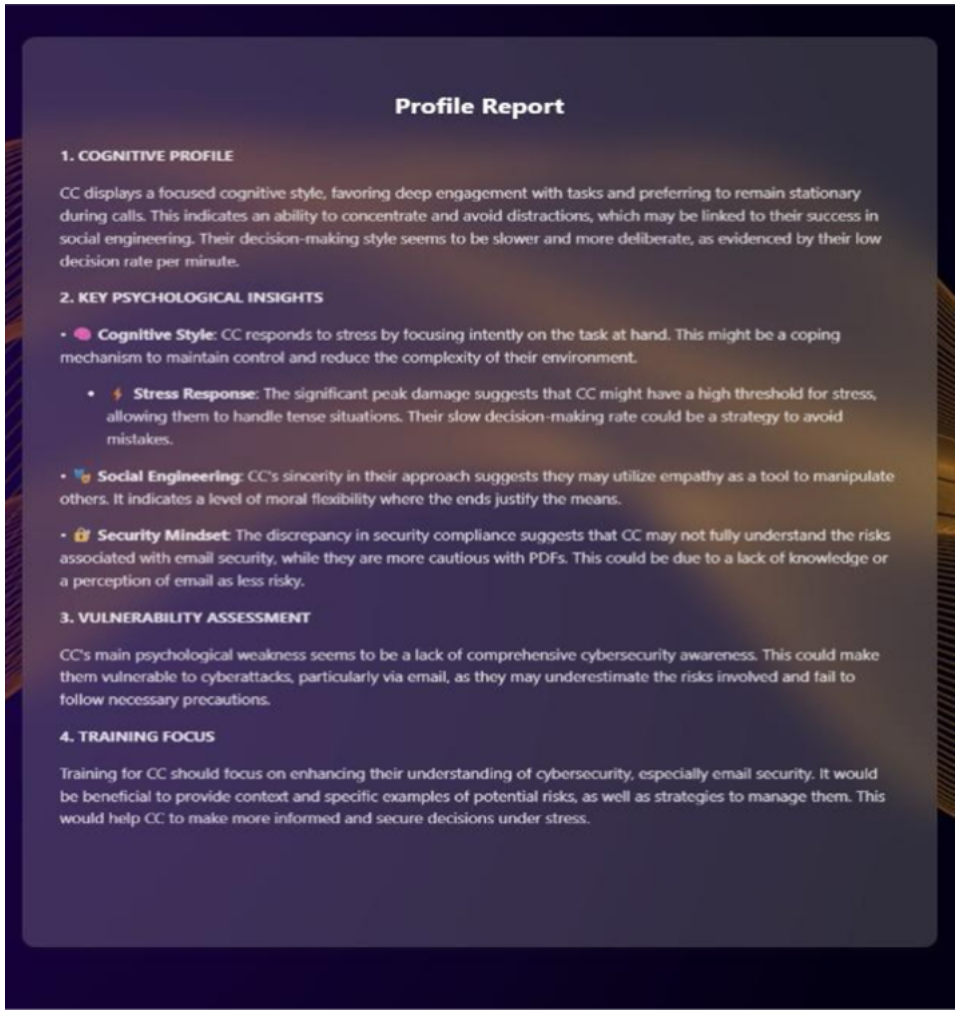
Thanks to the aid of Deep Fake technology the employee thinks he's having a conversation with the CFO that leads him to download and open a malicious pdf that injects a ransomware.

Cyber competence gap, qualcosa è cambiato
Results





Cyber competence gap, qualcosa è cambiato
Results



Profile Report

1. COGNITIVE PROFILE

CC displays a focused cognitive style, favoring deep engagement with tasks and preferring to remain stationary during calls. This indicates an ability to concentrate and avoid distractions, which may be linked to their success in social engineering. Their decision-making style seems to be slower and more deliberate, as evidenced by their low decision rate per minute.

2. KEY PSYCHOLOGICAL INSIGHTS

- **Cognitive Style**: CC responds to stress by focusing intently on the task at hand. This might be a coping mechanism to maintain control and reduce the complexity of their environment.
  - **Stress Response**: The significant peak damage suggests that CC might have a high threshold for stress, allowing them to handle tense situations. Their slow decision-making rate could be a strategy to avoid mistakes.
- **Social Engineering**: CC's sincerity in their approach suggests they may utilize empathy as a tool to manipulate others. It indicates a level of moral flexibility where the ends justify the means.
- **Security Mindset**: The discrepancy in security compliance suggests that CC may not fully understand the risks associated with email security, while they are more cautious with PDFs. This could be due to a lack of knowledge or a perception of email as less risky.

3. VULNERABILITY ASSESSMENT

CC's main psychological weakness seems to be a lack of comprehensive cybersecurity awareness. This could make them vulnerable to cyberattacks, particularly via email, as they may underestimate the risks involved and fail to follow necessary precautions.

4. TRAINING FOCUS

Training for CC should focus on enhancing their understanding of cybersecurity, especially email security. It would be beneficial to provide context and specific examples of potential risks, as well as strategies to manage them. This would help CC to make more informed and secure decisions under stress.

KPIs Derived from the Report

Attention and Cognitive Focus

- **Concentration Index: High** (Based on preference for stationary environments and focused task engagement)
- **Decision-Making Speed: Low, but deliberate**(Useful for in-depth analysis but may be slow in urgent contexts)

Stress Management

- **Stress Tolerance Threshold: High** (Demonstrated by the ability to operate in tense situations)

Social Risk Propensity

- **Vulnerability to Social Engineering: Moderate** (Due to empathy and sincerity, which can be exploited by attackers)

Security Awareness

- **Security Compliance Score: Low** (Indicates the user may not fully understand risks related to digital content like PDFs)

Security Behavior

- **Vulnerability to Phishing/Spear Phishing: High** (Due to lack of awareness about common attack vectors)